



Splunk

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 1)

A space is an implied _____ in a search string.

- A. OR
- B. AND
- C. ()
- D. NOT

Answer: B

Explanation:

A space is an implied AND in a search string, which means that it acts as a logical operator that returns events that match both terms on either side of the space. For example, `status=200 method=GET` will return event that have both `status=200` and `method=GET`. Therefore, option B is correct, while options A, C and D are incorrect because they are not implied by a space in a search string.

NEW QUESTION 2

- (Exam Topic 1)

When should you use the transaction command instead of the stats command?

- A. When you need to group on multiple values.
- B. When duration is irrelevant in search result
- C. .
- D. When you have over 1000 events in a transaction.
- E. When you need to group based on start and end constraints.

Answer: D

Explanation:

The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command can also specify start and end constraints for the transactions, such as a field value that indicates the beginning or the end of a transaction. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command cannot group events based on start and end constraints, but only on fields or time buckets. Therefore, the transaction command should be used instead of the stats command when you need to group events based on start and end constraints.

NEW QUESTION 3

- (Exam Topic 1)

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases can be used in lookup file definitions.
- C. Field aliases only normalize data across sources and sourcetypes.
- D. Field alias names are not case sensitive when used as part of a search.

Answer: B

Explanation:

Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for `src_ip` that maps to `clientip`, `source_address`, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for `src_ip` to map it to `ip_address` in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that `src_ip` and `SRC_IP` are different fields.

NEW QUESTION 4

- (Exam Topic 1)

Which of the following actions can the eval command perform?

- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

Answer: B

Explanation:

The eval command is used to create new fields or modify existing fields based on an expression. The eval command can perform various actions such as calculations, conversions, string manipulations and more. One of the actions that the eval command can perform is to create or replace an existing field with a new value based on an expression. For example, `| eval status=if(status="200","OK","ERROR")` will create or replace status field with either OK or ERROR depending on the original value of status. Therefore, option B is correct, while options A, C and D are incorrect because they are not actions that the eval command can perform.

NEW QUESTION 5

- (Exam Topic 1)

Which of the following searches show a valid use of macro? (Select all that apply)

- A. `index=main source=mySource oldField=* |'makeMyField(oldField)' | table _time newField`

- B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField
C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)' | table _time newField
D. index=main source=mySource oldField=* | "newField('makeMyField(oldField)') | table _time newField

Answer: AC

Explanation:

Reference:

<https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html>

To use a macro in a search, you must enclose the macro name and any arguments in single quotation marks¹. For example, 'my_macro(arg1,arg2)' is a valid way to use a macro with two arguments. You can use macro anywhere in your search string where you would normally use a search command or expression¹.

Therefore, options A and C are valid searches that use macros, while options B and D are invalid because they do not enclose the macros in single quotation marks.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following Statements about macros is true? (select all that apply)

- A. Arguments are defined at execution time.
B. Arguments are defined when the macro is created.
C. Argument values are used to resolve the search string at execution time.
D. Argument values are used to resolve the search string when the macro is created.

Answer: BC

Explanation:

A macro is a way to save a commonly used search string as a variable that you can reuse in other searches¹. When you create a macro, you can define arguments that are placeholders for values that you specify at execution time¹. The argument values are used to resolve the search string when the macro is invoked, not when it is created¹. Therefore, statements B and C are true, while statements A and D are false.

NEW QUESTION 7

- (Exam Topic 1)

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. Fast mode is enabled.
B. The dashboard is private.
C. The extraction is private
D. The person in the organization running the report does not have access to the index.

Answer: CD

Explanation:

The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface². You can create a report using a custom field extracted by the FX and share it with other users in your organization². However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field². To make the extraction available to other users, you need to make it global or app-level². Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored². To fix this issue, you need to grant the appropriate permissions to the other user for the index². Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

NEW QUESTION 8

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
B. Search workflow actions will run as a real-time search.
C. Search workflow actions can be configured as scheduled searches,
D. The user can define the time range of the search when created the workflow action.
E. Search workflow actions cannot be configured with a search string that includes the transaction command

Answer: C

Explanation:

Search workflow actions are custom actions that run a search when you click on a field value in your search results. Search workflow actions can be configured with various options, such as label name, search string, time range, app context, etc. One of the options is to define the time range of the search when creating the workflow action. You can choose from predefined time ranges, such as Last 24 hours, Last 7 days, etc., or specify a custom time range using relative or absolute time modifiers. Search workflow actions do not run as real-time searches by default, but rather use the same time range as the original search unless specified otherwise. Search workflow actions cannot be configured as scheduled searches, as they are only triggered by user interaction. Search workflow actions can be configured with any valid search string that includes any search command, such as transaction.

NEW QUESTION 9

- (Exam Topic 1)

Which of the following can be used with the eval command tostring function (select all that apply)

- A. "hex"
B. "commas"
C. "Decimal"
D. "duration"

Answer: ABD

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY> The tostring function in the eval command converts a numeric value to a string value. It can take an optional second argument that specifies the format of the string value. Some of the possible formats are:

- hex: converts the numeric value to a hexadecimal string.
- commas: adds commas to separate thousands in the numeric value.
- duration: converts the numeric value to a human-readable duration string, such as “2h 3m 4s”. Therefore, the formats A, B, and D can be used with the tostring function.

NEW QUESTION 10

- (Exam Topic 1)

Which of the following statements describes macros?

- A. A macro is a reusable search string that must contain the full search.
- B. A macro is a reusable search string that must have a fixed time range.
- C. A macro is a reusable search string that may have a flexible time range.
- D. A macro is a reusable search string that must contain only a portion of the search.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

A macro is a reusable search string that can contain any part of a search, such as search terms, commands, arguments, etc. A macro can have a flexible time range that can be specified when the macro is executed. A macro can also have arguments that can be passed to the macro when it is executed. A macro can be created by using the Settings menu or by editing the macros.conf file. A macro does not have to contain the full search, but only the part that needs to be reused. A macro does not have to have a fixed time range, but can use a relative or absolute time range modifier. A macro does not have to contain only a portion of the search, but can contain multiple parts of the search.

NEW QUESTION 10

- (Exam Topic 1)

After manually editing a regular expression (regex), which of the following statements is true?

- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

Answer: B

Explanation:

After manually editing a regular expression (regex) that was created using the Field Extractor (FX) UI, it is no longer possible to edit the field extraction in the FX UI. The FX UI is a tool that helps you extract fields from your data using delimiters or regular expressions. The FX UI can generate a regex for you based on your selection of sample values or you can enter your own regex in the FX UI. However, if you edit the regex manually in the props.conf file, the FX UI will not be able to recognize the changes and will not let you edit the field extraction in the FX UI anymore. You will have to use the props.conf file to make any further changes to the field extraction. Changes made manually cannot be reverted in the FX UI, as the FX UI does not keep track of the changes made in the props.conf file. It is possible to manually edit a regex that was created using the FX UI, as long as you do it in the props.conf file. Therefore, only statement B is true about manually editing a regex.

NEW QUESTION 15

- (Exam Topic 1)

Which of the following statements about data models and pivot are true? (select all that apply)

- A. They are both knowledge objects.
- B. Data models are created out of datasets called pivots.
- C. Pivot requires users to input SPL searches on data models.
- D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Answer: D

Explanation:

Data models and pivot are both knowledge objects in Splunk that allow you to analyze and visualize your data in different ways. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivot is a user interface that allows you to create data visualizations that present different aspects of a data model. Pivot does not require users to input SPL searches on data models, but rather lets them select options from menus and forms. Data models are not created out of datasets called pivots, but rather pivots are created from datasets in data models.

NEW QUESTION 18

- (Exam Topic 1)

Data model are composed of one or more of which of the following datasets? (select all that apply.)

- A. Events datasets
- B. Search datasets
- C. Transaction datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels>

Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:

Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.

Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.

Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

NEW QUESTION 20

- (Exam Topic 1)

How does a user display a chart in stack mode?

- A. By using the stack command.
- B. By turning on the Use Trellis Layout option.
- C. By changing Stack Mode in the Format menu.
- D. You cannot display a chart in stack mode, only a timechart.

Answer: C

Explanation:

A chart is a graphical representation of your search results that shows the relationship between two or more fields². You can display a chart in stack mode by changing the Stack Mode option in the Format menu². Stack mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series². Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

NEW QUESTION 21

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) `Sourcetype=access_combined | transaction JSESSIONID`

- A. An additional field named maxspan is created.
- B. An additional field named duration is created.
- C. An additional field named eventcount is created.
- D. Events with the same JSESSIONID will be grouped together into a single event.

Answer: BCD

Explanation:

The command `sourcetype=access_combined | transaction JSESSIONID` does three things:

- It filters the events by the sourcetype `access_combined`, which is a predefined sourcetype for Apache web server logs.
 - It groups the events by the field `JSESSIONID`, which is a unique identifier for each user session.
 - It creates a single event from each group of events that share the same `JSESSIONID` value. This single event will have some additional fields created by the transaction command, such as `duration`, `eventcount`, and `starttime`.
- Therefore, the statements B, C, and D are true.

NEW QUESTION 24

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XMI attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: C

Explanation:

POST workflow actions are custom actions that send a POST request to a web server when you click on a field value in your search results. POST workflow actions can be configured with various options, such as label name, base URL, URI parameters, post arguments, app context, etc. One of the options that are required to create a POST workflow action is post arguments. Post arguments are key-value pairs that are sent in the body of the POST request to provide additional information to the web server. Post arguments can include field values from your data by using dollar signs around the field names.

NEW QUESTION 28

- (Exam Topic 1)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields>

A calculated field is a field that you create based on the value of another field or fields¹. You can use calculated fields to enrich your data with additional

information or to transform your data into a more useful format¹. Calculated fields can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters, or key-value pairs¹. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

NEW QUESTION 31

- (Exam Topic 1)

A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B

Explanation:

As mentioned before, a calculated field is a field that you create based on the value of another field or fields². A calculated field can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

NEW QUESTION 34

- (Exam Topic 1)

Which of the following statements describe data model acceleration? (select all that apply)

- A. Root events cannot be accelerated.
- B. Accelerated data models cannot be edited.
- C. Private data models cannot be accelerated.
- D. You must have administrative permissions or the `accelerate_dacamodel` capability to accelerate a data model.

Answer: BCD

Explanation:

Data model acceleration is a feature that speeds up searches on data models by creating and storing summaries of the data model datasets¹. To enable data model acceleration, you must have administrative permissions or the `accelerate_datamodel` capability¹. Therefore, option D is correct. Accelerated data models cannot be edited unless you disable the acceleration first¹. Therefore, option B is correct. Private data models cannot be accelerated because they are not visible to other users¹. Therefore, option C is correct. Root events can be accelerated as long as they are not based on a search string¹. Therefore, option A is incorrect.

NEW QUESTION 39

- (Exam Topic 1)

In what order are the following knowledge objects/configurations applied?

- A. Field Aliases, Field Extractions, Lookups
- B. Field Extractions, Field Aliases, Lookups
- C. Field Extractions, Lookups, Field Aliases
- D. Lookups, Field Aliases, Field Extractions

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge> Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze². Some examples of knowledge objects are field extractions, field aliases and lookups². Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs². Field aliases are ways to assign alternative names to existing fields without changing the original field names or values². Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases². The order in which these knowledge objects/configurations are applied is as follows: field extractions, field aliases and then lookups². This means that Splunk first extracts fields from your raw data, then applies any aliases to the extracted fields and then performs any lookups on the aliased fields². Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 40

- (Exam Topic 1)

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

- A. `Index-main | REJECT trans sessionid`
- B. `Index-main | transaction sessionid | search REJECT`
- C. `Index=main | transaction sessionid | whose transaction=reject`
- D. `Index=main | transaction sessionid | where transaction=reject`

Answer: B

Explanation:

The transaction command is used to group events that share a common value for one or more fields into transactions². The transaction command assigns a transaction ID to each group of events and creates new fields such as `duration`, `eventcount` and `eventlist` for each transaction². To identify all of the contributing events within a transaction that contains at least one REJECT event, you can use the following syntax: `index=main | transaction sessionid | search REJECT`². This search will first group the events by `sessionid`, then filter out the transactions that do not contain REJECT in any of their events². Therefore, option B is correct, while options A, C and D are incorrect because they do not follow the correct syntax for using the transaction command or the search command.

NEW QUESTION 41

- (Exam Topic 1)

What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

- A. Macros.
- B. Field aliases.
- C. The rename command.
- D. CIM does not work with different names for the same field.

Answer: B

Explanation:

The Splunk Common Information Model (CIM) add-on helps you normalize your data from different sources and make it easier to analyze and report on it³. One of the functionalities that the CIM add-on relies on to normalize fields with different names is field aliases³. Field aliases allow you to assign an alternative name to an existing field without changing the original field name or value². By using field aliases, you can map different field names from different sources or sourcetypes to a common field name that conforms to the CIM standard³. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 44

- (Exam Topic 1)

Which of the following statements describes this search? `sourcetype=access_combined | transaction JSESSIONID | timechart avg (duration)`

- A. This is a valid search and will display a timechart of the average duration, of each transaction event.
- B. This is a valid search and will display a stats table showing the maximum pause among transactions.
- C. No results will be returned because the transaction command must include the startswith and endswith options.
- D. No results will be returned because the transaction command must be the last command used in the search pipeline.

Answer: A

Explanation:

This search uses the transaction command to group events that share a common value for JSESSIONID into transactions¹. The transaction command assigns a duration field to each transaction, which is the difference between the latest and earliest timestamps of the events in the transaction¹. The search then uses the timechart command to create a time-series chart of the average duration of each transaction¹. Therefore, option A is correct because it describes the search accurately. Option B is incorrect because the search does not use the stats command or the pause field. Option C is incorrect because the transaction command does not require the startswith and endswith options, although they can be used to specify how to identify the beginning and end of a transaction¹. Option D is incorrect because the transaction command does not have to be the last command in the search pipeline, although it is often used near the end of a search¹.

NEW QUESTION 49

- (Exam Topic 1)

What are the two parts of a root event dataset?

- A. Fields and variables.
- B. Fields and attributes.
- C. Constraints and fields.
- D. Constraints and lookups.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkLight/7.3.5/GettingStarted/Design/datamodelobjects> A root event dataset is the base dataset for a data model that defines the source or sources of the data and the constraints and fields that apply to the data¹. A root event dataset has two parts: constraints and fields¹. Constraints are filters that limit the data to a specific index, source, sourcetype, host or search string¹. Fields are the attributes that describe the data and can be extracted, calculated or looked up¹. Therefore, option C is correct, while options A, B and D are incorrect.

NEW QUESTION 52

- (Exam Topic 1)

Which of the following statements about event types is true? (select all that apply)

- A. Event types can be tagged.
- B. Event types must include a time range.
- C. Event types categorize events based on a search.
- D. Event types can be a useful method for capturing and sharing knowledge.

Answer: ACD

Explanation:

Reference: <https://www.edureka.co/blog/splunk-events-event-types-and-tags/>

As mentioned before, an event type is a way to categorize events based on a search string that matches the events². Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches². Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type². Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization². Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events². Therefore, option B is incorrect.

NEW QUESTION 55

- (Exam Topic 1)

Which of the following workflow actions can be executed from search results? (select all that apply)

- A. GET
- B. POST

- C. LOOKUP
- D. Search

Answer: ABD

Explanation:

As mentioned before, there are two types of workflow actions: GET and POST¹. Both types of workflow actions can be executed from search results by clicking on an event field value that has a workflow action configured for it¹. Another type of workflow action is Search, which runs another search based on the field value¹. Therefore, options A, B and D are correct, while option C is incorrect because LOOKUP is not a type of workflow action.

NEW QUESTION 59

- (Exam Topic 1)

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.
- D. The CIM add-on is automatically installed in a Splunk environment.

Answer: C

Explanation:

The Splunk Common Information Model (CIM) add-on is a Splunk app that contains data models to help you normalize data from different sources and formats. The CIM add-on defines a common and consistent way of naming and categorizing fields and events in Splunk. This makes it easier to correlate and analyze data across different domains, such as network, security, web, etc. The CIM add-on does not use machine learning to normalize data, but rather relies on predefined field names and values. The CIM add-on does not contain dashboards that show how to map data, but rather provides documentation and examples on how to use the data models. The CIM add-on is not automatically installed in a Splunk environment, but rather needs to be downloaded and installed from Splunkbase.

NEW QUESTION 60

- (Exam Topic 1)

What is the relationship between data models and pivots?

- A. Data models provide the datasets for pivots.
- B. Pivots and data models have no relationship.
- C. Pivots and data models are the same thing.
- D. Pivots provide the datasets for data models.

Answer: A

Explanation:

The relationship between data models and pivots is that data models provide the datasets for pivots. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivots are user interfaces that allow you to create data visualizations that present different aspects of a data model. Pivots let you select options from menus and forms to create charts, tables, maps, etc., without writing any SPL code. Pivots use datasets from data models as their source of data. Pivots and data models are not the same thing, as pivots are tools for visualizing data models. Pivots do not provide datasets for data models, but rather use them as inputs. Therefore, only statement A is true about the relationship between data models and pivots.

NEW QUESTION 61

- (Exam Topic 2)

This function of the stats command allows you to return the middle-most value of field X.

- A. Median(X)
- B. Eval by X
- C. Fields(X)
- D. Values(X)

Answer: A

NEW QUESTION 62

- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

Answer: C

Explanation:

The search modes determine how Splunk processes your search and displays your results². There are three search modes: Fast, Smart and Verbose². The search mode that automatically returns all extracted fields in the fields sidebar is Verbose². The Verbose mode shows all the fields that are extracted from your events, including default fields, indexed fields and search-time extracted fields². The fields sidebar is a panel that shows the fields that are present in your search results². Therefore, option C is correct, while options A and B are incorrect because they are not search modes that automatically return all extracted fields in the fields sidebar.

NEW QUESTION 63

- (Exam Topic 2)

What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?

- A. Consult the CIM data model reference tables.
- B. Run a search using the authentication command.
- C. Consult the CIM event type reference tables.
- D. Run a search using the correlation command.

Answer: A

Explanation:

The recommended approach when using the Splunk Common Information Model (CIM) add-on to normalize data is A. Consult the CIM data model reference tables. This is because the CIM data model reference tables provide detailed information about the fields and tags that are expected for each dataset in a data model. By consulting the reference tables, you can determine which data models are relevant for your data source and how to map your data fields to the CIM fields. You can also use the reference tables to validate your data and troubleshoot any issues with normalization. You can find the CIM data model reference tables in the Splunk documentation¹ or in the Data Model Editor page in Splunk Web². The other options are incorrect because they are not related to the CIM add-on or data normalization. The authentication command is a custom command that validates events against the Authentication data model, but it does not help you to normalize other types of data. The correlation command is a search command that performs statistical analysis on event fields, but it does not help you to map your data fields to the CIM fields. The CIM event type reference tables do not exist, as event types are not part of the CIM add-on.

NEW QUESTION 67

- (Exam Topic 2)

When using the transaction command, how are evicted transactions identified?

- A. Closed_txn field is set to 0, or false.
- B. Max_txn field is set to 0, or false.
- C. Txn_field is set to 1, or true.
- D. open_txn field is set to 1, or true.

Answer: A

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints¹.
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member¹.
- The transaction command adds some fields to the raw events that are part of the transaction¹². These fields are:
 - duration: The difference, in seconds, between the timestamps for the first and last events in the transaction¹².
 - eventcount: The number of events in the transaction¹².
 - closed_txn: A Boolean field that indicates whether the transaction is closed or evicted². A transaction is closed if it meets one of the following conditions: maxevents, maxpause, maxsp or startswith². A transaction is evicted if it does not meet any of these conditions and exceeds the memory limit specified by maxopentxn or maxopenevents²³.
- Therefore, evicted transactions can be distinguished from non-evicted transactions by checking the value of the closed_txn field. The closed_txn field is set to 0, or false, for evicted transactions and 1 for non-evicted, or closed, transactions²³.

NEW QUESTION 70

- (Exam Topic 2)

What type of command is eval?

- A. Streaming in some modes
- B. Report generating
- C. Distributable streaming
- D. Centralized streaming

Answer: C

Explanation:

The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation¹.

NEW QUESTION 73

- (Exam Topic 2)

The eval command 'if' function requires the following three arguments (in order):

- A. Boolean expression, result if true, result if false
- B. Result if true, result if false, boolean expression
- C. Result if false, result if true, boolean expression
- D. Boolean expression, result if false, result if true

Answer: A

Explanation:

The eval command 'if' function requires the following three arguments (in order): boolean expression, result if true, result if false. The eval command is a search command that allows you to create new fields or modify existing fields by performing calculations or transformations on them. The eval command can use various functions to perform different operations on fields. The 'if' function is one of the functions that can be used with the eval command to perform conditional evaluations on fields. The 'if' function takes three arguments: a boolean expression that evaluates to true or false, a result that will be returned if the boolean expression is true, and a result that will be returned if the boolean expression is false. The 'if' function returns one of the two results based on the evaluation of

the boolean expression.

NEW QUESTION 77

- (Exam Topic 2)

Field aliases are used to _____ data

- A. clean
- B. transform
- C. calculate
- D. normalize

Answer: D

NEW QUESTION 81

- (Exam Topic 2)

Which field extraction method should be selected for comma-separated data?

- A. Regular expression
- B. Delimiters
- C. eval expression
- D. table extraction

Answer: B

Explanation:

The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation¹. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation²³.

NEW QUESTION 83

- (Exam Topic 2)

Using the export function, you can export search results as _____. (Select all that apply)

- A. Xml
- B. Json
- C. Html
- D. A php file

Answer: AB

Explanation:

Using the export function, you can export search results as XML or JSON². The export function allows you to save your search results in a structured format that can be used by other applications or tools². You can use the output_mode parameter to specify whether you want to export your results as XML or JSON². Therefore, options A and B are correct, while options C and D are incorrect because they are not formats that you can export your search results as.

NEW QUESTION 87

- (Exam Topic 2)

When using the timechart command, how can a user group the events into buckets based on time?

- A. Using the span argument.
- B. Using the duration argument.
- C. Using the interval argument.
- D. Adjusting the fieldformat options.

Answer: A

NEW QUESTION 90

- (Exam Topic 2)

Which command is used to create choropleth maps?

- A. geostats
- B. cluster
- C. geom

Answer: C

NEW QUESTION 91

- (Exam Topic 2)

We can use the rename command to _____ (Select all that apply.)

- A. Change indexed fields
- B. Exclude fields from our search results
- C. Extract new fields from our data using regular expressions

D. Give a field a new name at search time

Answer: D

NEW QUESTION 95

- (Exam Topic 2)

The transaction command allows you to _____ events across multiple sources

- A. duplicate
- B. correlate
- C. persist
- D. tag

Answer: B

Explanation:

The transaction command allows you to correlate events across multiple sources. The transaction command is a search command that allows you to group events into transactions based on some common characteristics, such as fields, time, or both. A transaction is a group of events that share one or more fields that relate them to each other. A transaction can span across multiple sources or sourcetypes that have different formats or structures of data. The transaction command can help you correlate events across multiple sources by using the common fields as the basis for grouping. The transaction command can also create some additional fields for each transaction, such as duration, eventcount, starttime, etc.

NEW QUESTION 99

- (Exam Topic 2)

Information needed to create a GET workflow action includes which of the following? (select all that apply.)

- A. A name of the workflow action
- B. A URI where the user will be directed at search time.
- C. A label that will appear in the Event Action menu at search time.
- D. A name for the URI where the user will be directed at search time.

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/SetupaGETworkflowaction> Information needed to create a GET workflow action includes the following: a name of the workflow action, a URI where the user will be directed at search time, and a label that will appear in the Event Action menu at search time. A GET workflow action is a type of workflow action that performs a GET request when you click on a field value in your search results. A GET workflow action can be configured with various options, such as:

A name of the workflow action: This is a unique identifier for the workflow action that is used internally by Splunk. The name should be descriptive and meaningful for the purpose of the workflow action.

A URI where the user will be directed at search time: This is the base URL of the external web service or application that will receive the GET request. The URI can include field value variables that will be replaced by the actual field values at search time. For example, if you have a field value variable ip, you can write it as [http://example.com/ip=\\$ip](http://example.com/ip=$ip) to send the IP address as a parameter to the external web service or application.

A label that will appear in the Event Action menu at search time: This is the display name of the workflow action that will be shown in the Event Action menu when you click on a field value in your search results. The label should be clear and concise for the user to understand what the workflow action does.

Therefore, options A, B, and C are correct.

NEW QUESTION 102

- (Exam Topic 2)

A data model can consist of what three types of datasets?

- A. Pivot, searches, and events.
- B. Pivot, events, and transactions.
- C. Searches, transactions, and pivot.
- D. Events, searches, and transactions.

Answer: D

NEW QUESTION 107

- (Exam Topic 2)

This clause is used to group the output of a stats command by a specific name.

- A. Rex
- B. As
- C. List
- D. By

Answer: B

NEW QUESTION 108

- (Exam Topic 2)

Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

- A. inputlookup
- B. lookup

Answer: B

NEW QUESTION 109

- (Exam Topic 2)

Data models are composed of one or more of which of the following datasets? (select all that apply)

- A. Transaction datasets
- B. Events datasets
- C. Search datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

Explanation:

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

<https://docs.splunk.com/Splexicon:Datamodeldataset>

NEW QUESTION 114

- (Exam Topic 2)

What commands can be used to group events from one or more data sources?

- A. eval, coalesce
- B. transaction, stats
- C. stats, format
- D. top, rare

Answer: B

Explanation:

The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events. The top and rare commands are used to rank the most or least common values of a field, not to group events²³

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command. 3: Splunk Documentation, stats command.

NEW QUESTION 119

- (Exam Topic 2)

What is the Splunk Common Information Model (CIM)?

- A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.
- B. The CIM provides a methodology to normalize data from different sources and source types.
- C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.
- D. The CIM is a data exchange initiative between software vendors.

Answer: B

Explanation:

The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

NEW QUESTION 121

- (Exam Topic 2)

What other syntax will produce exactly the same results as | chart count over vendor_action by user?

- A. | chart count by vendor_action, user
- B. | chart count over vendor_action, user
- C. | chart count by vendor_action over user
- D. | chart count over user by vendor_action

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart>

NEW QUESTION 122

- (Exam Topic 2)

Which of the following commands support the same set of functions?

- A. stats, eval, table
- B. search, where, eval
- C. stats, chart, timechart
- D. transaction, chart, timechart

Answer: C

NEW QUESTION 123

- (Exam Topic 2)

Which workflow action method can be used the action type is set to link?

- A. GET
- B. PUT
- C. Search
- D. UPDATE

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/SetupaGETworkflowaction>

Define a GET workflow action

Steps

- Navigate to Settings > Fields > Workflow Actions.
- Click New to open up a new workflow action form.
- Define a Label for the action.

The Label field enables you to define the text that is displayed in either the field or event workflow menu.

Labels can be static or include the value of relevant fields.

- Determine whether the workflow action applies to specific fields or event types in your data.

Use Apply only to the following fields to identify one or more fields. When you identify fields, the workflow

action only appears for events that have those fields, either in their event menu or field menus. If you leave it blank or enter an asterisk the action appears in menus for all fields.

Use Apply only to the following event types to identify one or more event types. If you identify an event type, the workflow action only appears in the event menus for events that belong to the event type.

- For Show action in determine whether you want the action to appear in the Event menu, the Fields menus, or Both.
- Set Action type to link.
- In URI provide a URI for the location of the external resource that you want to send your field values to.

Similar to the Label setting, when you declare the value of a field, you use the name of the field enclosed by dollar signs.

Variables passed in GET actions via URIs are automatically URL encoded during transmission. This means you can include values that have spaces between words or punctuation characters.

- Under Open link in, determine whether the workflow action displays in the current window or if it opens the link in a new window.
- Set the Link method to get.
- Click Save

to save your workflow action definition.

NEW QUESTION 126

- (Exam Topic 2)

What happens when a user edits the regular expression (regex) field extraction generated in the Field Extractor (FX)?

- A. There is a limit to the number of fields that can be extracted.
- B. The user is unable to preview the extractions.
- C. The extraction is added at index time.
- D. The user is unable to return to the automatic field extraction workflow.

Answer: A

NEW QUESTION 129

- (Exam Topic 2)

Which of the following statements describes calculated fields?

- A. Calculated fields are only used on fields added by lookups.
- B. Calculated fields are a shortcut for repetitive and complex eval commands.
- C. Calculated fields are a shortcut for repetitive and complex calc commands.
- D. Calculated fields automatically calculate the simple moving average for indexed fields.

Answer: B

NEW QUESTION 131

- (Exam Topic 2)

Which of these search strings is NOT valid:

- A. index=web status=50* | chart count over host, status
- B. index=web status=50* | chart count over host by status
- C. index=web status=50* | chart count by host, status

Answer: A

Explanation:

This search string is not valid: index=web status=50* | chart count over host,status2. This search string uses an invalid syntax for the chart command. The chart command requires one field after the over clause and optionally one field after the by clause. However, this search string has two fields after the over clause separated by a comma. This will cause a syntax error and prevent the search from running. Therefore, option A is correct, while options B and C are incorrect because they are valid search strings that use the chart command correctly.

NEW QUESTION 133

- (Exam Topic 2)

Which method in the Field Extractor would extract the port number from the following event?

| 10/20/2022 - 125.24.20.1 ++++ port 54 - user: admin <web error>

- A. Delimiter
- B. rex command
- C. The Field Extractor tool cannot extract regular expressions.
- D. Regular expression

Answer: B

Explanation:

The rex command allows you to extract fields from events using regular expressions. You can use the rex command to specify a named group that matches the port number in the event. For example:

rex "\+\\+\\+port (?<port>\\d+)"

This will create a field called port with the value 54 for the event.

The delimiter method is not suitable for this event because there is no consistent delimiter between the fields. The regular expression method is not a valid option for the Field Extractor tool. The Field Extractor tool can extract regular expressions, but it is not a method by itself.

Reference: 1

Splunk Core Certified Power User | Splunk

NEW QUESTION 134

- (Exam Topic 2)

For the following search, which field populates the x-axis? index=security sourcetype=linux secure | timechart count by action

- A. action
- B. source type
- C. _time
- D. time

Answer: C

Explanation:

The correct answer is C. _time.

The timechart command creates a time series chart with corresponding table of statistics, with time used as the X-axis¹. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart¹. In this case, the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail². The count function will calculate the number of events for each action in each time bin¹.

For example, the following image shows a timechart of the count by action for a similar search³:

As you can see, the x-axis is populated by the _time field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different values of the action field, which are used to split the chart into different series.

Reference:

2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

NEW QUESTION 136

- (Exam Topic 2)

Which of the following statements describes the use of the Field Extractor (FX)?

- A. The Field Extractor automatically extracts all fields at search time.
- B. The Field Extractor uses PERL to extract fields from the raw events.
- C. Fields extracted using the Field Extractor persist as knowledge objects.
- D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C

Explanation:

The statement that fields extracted using the Field Extractor persist as knowledge objects is true. The Field Extractor (FX) is a graphical tool that allows you to extract fields from raw events using regular expressions or delimiters. The fields extracted by the FX are saved as knowledge objects that can be used in future searches or shared with other users.

NEW QUESTION 141

- (Exam Topic 2)

Which of the following statements are true for this search? (Select all that apply.)

SEARCH: sourcetype=access* |fields action productId status

- A. is looking for all events that include the search terms: fields AND action AND productId AND status
- B. users the table command to improve performance
- C. limits the fields are extracted
- D. returns a table with 3 columns

Answer: C

NEW QUESTION 144

- (Exam Topic 2)

Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

- A. POST
- B. Search
- C. GET
- D. Format

Answer: A

Explanation:

The type of workflow action that sends field values to an external resource (e.g. a ticketing system) is POST. A POST workflow action allows you to send a POST request to a URI location with field values or static values as arguments. For example, you can use a POST workflow action to create a ticket in an external system with information from an event.

NEW QUESTION 149

- (Exam Topic 2)

Complete the search, | _____ failure>successes

- A. Search
- B. Where
- C. If
- D. Any of the above

Answer: B

Explanation:

The where command can be used to complete the search below.

... | where failure>successes

The where command is a search command that allows you to filter events based on complex or custom criteria. The where command can use any boolean expression or function to evaluate each event and determine whether to keep it or discard it. The where command can also compare fields or perform calculations on fields using operators such as >, <, =, +, -, etc. The where command can be used after any transforming command that creates a table or a chart.

The search string below does the following:

- It uses ... to represent any search criteria or commands before the where command.
- It uses the where command to filter events based on a comparison between two fields: failure and successes.
- It uses the greater than operator (>) to compare the values of failure and successes fields for each event.
- It only keeps events where failure is greater than successes.

NEW QUESTION 151

- (Exam Topic 2)

If a search returns _____ it can be viewed as a chart.

- A. timestamps
- B. statistics
- C. events
- D. keywords

Answer: B

Explanation:

If a search returns statistics, it can be viewed as a chart². Statistics are tabular data that show the relationship between two or more fields². You can create statistics by using commands such as stats, chart or timechart². You can view statistics as a chart by selecting the Visualization tab in the Search app and choosing a chart type such as column, line or pie². Therefore, option B is correct, while options A, C and D are incorrect because they are not types of data that can be viewed as a chart.

NEW QUESTION 155

- (Exam Topic 2)

Which of the following searches show a valid use of a macro? (Choose all that apply.)

- A. index=main source=mySource oldField=* |'makeMyField(oldField)'| table _time newField
- B. index=main source=mySource oldField=* | stats if('makeMyField(oldField)') | table _time newField
- C. index=main source=mySource oldField=* | eval newField='makeMyField(oldField)'| table _time newField
- D. index=main source=mySource oldField=* | "newField('makeMyField(oldField)')"' | table _time newField

Answer: AC

Explanation:

The searches A and C show a valid use of a macro. A macro is a reusable piece of SPL code that can be called by using single quotes ("). A macro can take arguments, which are passed inside parentheses after the macro name. For example, 'makeMyField(oldField)' calls a macro named makeMyField with an argument oldField. The searches B and D are not valid because they use double quotes ("") instead of single quotes (").

NEW QUESTION 159

- (Exam Topic 2)

Which of the following objects can a calculated field use as a source?

- A. An alias of a field.
- B. A field added by an automatic lookup.
- C. The tag field.
- D. The eventtype field.

Answer: B

Explanation:

The correct answer is B. A field added by an automatic lookup.

A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are

already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined¹.

An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field². An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields³.

Therefore, a calculated field can use a field added by an automatic lookup as a source. References:

- About calculated fields
- About lookups
- Search time processing

NEW QUESTION 162

- (Exam Topic 2)

How many ways are there to access the Field Extractor Utility?

- A. 3
- B. 4
- C. 1
- D. 5

Answer: A

NEW QUESTION 163

- (Exam Topic 2)

When creating a data model, which root dataset requires at least one constraint?

- A. Root transaction dataset
- B. Root event dataset
- C. Root child dataset
- D. Root search dataset

Answer: B

Explanation:

The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as `sourcetype=access_combined`. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation¹. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

NEW QUESTION 168

- (Exam Topic 2)

Why are tags useful in Splunk?

- A. Tags look for less specific data.
- B. Tags visualize data with graphs and charts.
- C. Tags group related data together.
- D. Tags add fields to the raw event data.

Answer: C

Explanation:

Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as `router`, and then search for `tag=router` to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values. For example, you can tag the field values `error`, `fail`, and `critical` as `severity=high`, and then search for `severity=high` to find all the events with high severity level².

1: Splunk Core Certified Power User Track, page 10. 2: Splunk Documentation, About tags and aliases.

NEW QUESTION 173

- (Exam Topic 2)

Which of the following eval command functions is valid?

- A. `int()`
- B. `count()`
- C. `print()`
- D. `tostring()`

Answer: D

Explanation:

<https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunctions>

The eval command function `tostring()` is valid. The `tostring()` function converts a numeric value to a string value. For example, `tostring(3.14)` returns "3.14". The other functions are not valid eval command functions.

NEW QUESTION 176

- (Exam Topic 2)

Which of the following searches would return a report of sales by product-name?

- A. chart sales by product_name
- B. chart sum(price) as sales by product_name
- C. stats sum(price) as sales over product_name
- D. timechart list(sales), values(product_name)

Answer: B

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Chart> <https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/Stats>

NEW QUESTION 180

- (Exam Topic 2)

Which of the following statements about calculated fields in Splunk is true?

- A. Calculated fields cannot be chained together to create more complex fields
- B. Calculated fields can be chained together to create more complex fields.
- C. Calculated fields can only be used in dashboards.
- D. Calculated fields can only be used in saved reports.

Answer: B

Explanation:

The correct answer is B. Calculated fields can be chained together to create more complex fields.

Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field¹.

Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as:

discount = total * 0.9

This will create a new field named discount that is equal to 90% of the total field value for each event². References:

- > [About calculated fields](#)
- > [Chaining calculated fields](#)

NEW QUESTION 185

- (Exam Topic 2)

How is an event type created from the search window? (select all that apply)

- A. In the top right corner, click Save As > Event Type.
- B. In an event's detail dropdown, click Event Actions > Build Event Type.
- C. Edit eventtypes.conf and add a new stanza.
- D. Add | eventtype to the SPL and execute the search.

Answer: AC

Explanation:

In Splunk, you can create an event type from the search window by running a search that would make a good event type, then clicking Save As and selecting Event Type¹. This opens the Save as Event Type dial you can provide the event type name and optionally apply tags to it¹.

You can also create an event type by editing the eventtypes.conf file and adding a new stanza¹. Each stanza in the eventtypes.conf file represents an event type¹.

The stanza name is the name of the event type, and

the search attribute specifies the search string that defines the event type¹.

It's important to note that while you can use the eventtype command in a search to find events associated with a specific event type, adding | eventtype to the SPL and executing the search does not create a new event type¹. Similarly, clicking Event Actions > Build Event Type in an event's detail dropdown does not create new event type¹.

NEW QUESTION 188

- (Exam Topic 2)

These users can create global knowledge objects. (Select all that apply.)

- A. users
- B. power users
- C. administrators

Answer: BC

NEW QUESTION 191

- (Exam Topic 2)

Which of the following is included with the Common Information Model (CIM) add-on?

- A. Search macros
- B. Event category tags
- C. Workflow actions
- D. tsidx files

Answer: B

Explanation:

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk documentation¹². The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

NEW QUESTION 192

- (Exam Topic 2)

These kinds of charts represent a series in a single bar with multiple sections

- A. Multi-Series
- B. Split-Series
- C. Omit nulls
- D. Stacked

Answer: D

Explanation:

Stacked charts represent a series in a single bar with multiple sections. A chart is a graphical representation of data that shows trends, patterns, or comparisons. A chart can have different types, such as column, bar, line, area, pie, etc. A chart can also have different modes, such as split-series, multi-series, stacked, etc. A stacked chart is a type of chart that shows multiple series in a single bar or area with different sections for each series

NEW QUESTION 194

- (Exam Topic 2)

This is what Splunk uses to categorize the data that is being indexed.

- A. Host
- B. Sourcetype
- C. Index
- D. Source

Answer: B

NEW QUESTION 199

- (Exam Topic 2)

If a calculated field has the same name as an extracted field, what happens to the extracted field?

- A. The calculated field will override the extracted field.
- B. The calculated and extracted fields will be combined.
- C. The calculated field will duplicate the extracted field.
- D. An error will be returned and the search will fail.

Answer: A

Explanation:

When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis. To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field²

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Configure calculated fields with props.conf.

NEW QUESTION 204

- (Exam Topic 2)

Which of the following are valid options to speed up reports? (Select all the apply.)

- A. Edit permissions
- B. Edit description
- C. Edit acceleration
- D. Edit schedule

Answer: C

Explanation:

One of the valid options to speed up reports is to edit acceleration, which means that you can enable summary indexing or data model acceleration for your reports to improve their performance². Summary indexing allows you to create reports that run over large amounts of data by storing the results of scheduled searches in a summary index and using that index for faster reporting². Data model acceleration allows you to create reports that use data models by creating and storing summaries of the data model datasets and using them for faster reporting². Therefore, option C is correct, while options A, B and D are incorrect because they are not options to speed up reports.

NEW QUESTION 208

- (Exam Topic 2)

When defining a macro, what are the required elements?

- A. Name and arguments.

- B. Name and a validation error message.
- C. Name and definition.
- D. Definition and arguments.

Answer: C

Explanation:

When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced. The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation.

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, Define search macros in Settings.

NEW QUESTION 212

- (Exam Topic 2)

When is a GET workflow action needed?

- A. To send field values to an external resource.
- B. To retrieve information from an external resource.
- C. To use field values to perform a secondary search.
- D. To define how events flow from forwarders to indexes.

Answer: B

NEW QUESTION 214

- (Exam Topic 2)

This function of the stats command allows you to return the sample standard deviation of a field.

- A. stdev
- B. dev
- C. count deviation
- D. by standarddev

Answer: A

NEW QUESTION 216

- (Exam Topic 2)

Which search would limit an "alert" tag to the "host" field?

- A. tag=alert
- B. host::tag::alert
- C. tag==alert
- D. tag::host=alert

Answer: D

Explanation:

The search below would limit an "alert" tag to the "host" field. tag::host=alert

The search does the following:

- It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data.
- It specifies tag::host=alert as the tag filter. This means that it will only return events that have an "alert" tag applied to their host field or host field value.
- It uses an equal sign (=) to indicate an exact match between the tag and the field or field value.

NEW QUESTION 218

- (Exam Topic 2)

Consider the following search: index=web sourcetype=access_corabined

The log shows several events that share the same jsessionid value (SD462K101O2F267). View the events as a group.

From the following list, which search groups events by JSESSIONID?

- A. index=web sourcetype=access_combined | transaction JSESSIONID | search SD462K101C2F267
- B. index=web sourcetype=access_combined SD462K101O2F267 | table JSESSIONID
- C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD462K101O2F267
- D. index=web sourcetype=access_combined JSESSIONID <SD462K101O2F267>

Answer: A

Explanation:

The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID.

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

NEW QUESTION 223

- (Exam Topic 2)

It is mandatory for the lookup file to have this for an automatic lookup to work.

- A. Source type

- B. At least five columns
- C. Timestamp
- D. Input filed

Answer: D

NEW QUESTION 226

- (Exam Topic 2)

Which is not a comparison operator in Splunk

- A. <=
- B. =
- C. !=
- D. >
- E. ?=

Answer: E

Explanation:

A comparison operator is a symbol that compares two values and returns a Boolean result (true or false)². Splunk supports various comparison operators such as <, >, =, !=, <=, >=, IN and LIKE². However, ?= is not a valid comparison operator in Splunk and will cause a syntax error if used in a search string². Therefore, option E is correct, while options A, B, C and D are incorrect because they are valid comparison operators in Splunk

NEW QUESTION 227

- (Exam Topic 2)

There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

- A. Event Actions > Extract Fields
- B. Fields sidebar > Extract New Field
- C. Settings > Field Extractions > New Field Extraction
- D. Settings > Field Extractions > Open Field Extraction

Answer: B

Explanation:

There are several ways to access the field extractor. The option that automatically identifies data type, source type, and sample event is Fields sidebar > Extract New Field. The field extractor is a tool that helps you extract fields from your data using delimiters or regular expressions. The field extractor can generate a regex for you based on your selection of sample values or you can enter your own regex in the field extractor. The field extractor can be accessed by using various methods, such as:

- Fields sidebar > Extract New Field: This is the easiest way to access the field extractor. The fields sidebar is a panel that shows all available fields for your data and their values. When you click on Extract New Field in the fields sidebar, Splunk will automatically identify the data type, source type, and sample event for your data based on your current search criteria. You can then use the field extractor to select sample values and generate a regex for your new field.
- Event Actions > Extract Fields: This is another way to access the field extractor. Event actions are actions that you can perform on individual events in your search results, such as viewing event details, adding to report, adding to dashboard, etc. When you click on Extract Fields in the event actions menu, Splunk will use the current event as the sample event for your data and ask you to select the source type and data type for your data. You can then use the field extractor to select sample values and generate a regex for your new field.
- Settings > Field Extractions > New Field Extraction: This is a more advanced way to access the field extractor. Settings is a menu that allows you to configure various aspects of Splunk, such as indexes, inputs, outputs, users, roles, apps, etc. When you click on New Field Extraction in the Settings menu, Splunk will ask you to enter all the details for your new field extraction manually, such as app context, name, source type, data type, sample event, regex, etc. You can then use the field extractor to verify or modify your regex for your new field.

NEW QUESTION 232

- (Exam Topic 2)

The fields sidebar does not show _____. (Select all that apply.)

- A. interesting fields
- B. selected fields
- C. all extracted fields

Answer: C

Explanation:

The fields sidebar is a panel that shows the fields that are present in your search results². The fields sidebar does not show all extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters or key-value pairs². The fields sidebar only shows selected fields and interesting fields². Selected fields are fields that you choose to display in your search results by clicking on them in the fields sidebar or by using the fields command². Interesting fields are fields that appear in at least 20 percent of events or have high variability among values². Therefore, option C is correct, while options A and B are incorrect because they are types of fields that the fields sidebar does show.

NEW QUESTION 233

- (Exam Topic 2)

Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

- A. Macros
- B. Lookups
- C. Workflow actions
- D. Field extractions

Answer: B

Explanation:

Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.
<https://docs.splunk.com/Documentation/CIM/4.15.0/User/UseTheCIMtonormalizedataatsearchtime>

NEW QUESTION 235

- (Exam Topic 2)

When extracting fields, we may choose to use our own regular expressions

- A. True
- B. False

Answer: A

NEW QUESTION 239

- (Exam Topic 2) Consider the following search: Index=web sourcetype=access_combined

The log shows several events that share the same JSESSIONID value (SD404K289O2F151). View the events as a group. From the following list, which search groups events by JSESSIONID?

- A. index=web sourcetype=access_combined SD404K289O2F151 | table JSESSIONID
- B. index=web sourcetype=access_combined JSESSIONID <SD404K289O2F151>
- C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD404K289O2F151
- D. index=web sourcetype=access_combined | transaction JSESSIONID | search SD404K289O2F151

Answer: B

NEW QUESTION 243

- (Exam Topic 2)

Which of the following statements about tags is true?

- A. Tags are case insensitive.
- B. Tags can make your data more understandable.
- C. Tags are created at index time.
- D. Tags are searched by using the syntax tag :: <fieldname>.

Answer: B

Explanation:

- Tags are a knowledge object that allow you to assign an alias to one or more field values . Tags are applied to events at search time and can be used as search terms or filters .
- Tags can help you make your data more understandable by replacing cryptic or complex field values with meaningful names . For example, you can tag the value 200 in the status field as success, or value 404 as not_found .

NEW QUESTION 247

- (Exam Topic 2)

Which of the following is a function of the Splunk Common Information Model (CIM)?

- A. Normalizing data across a Splunk deployment.
- B. Providing templates for reports and dashboards.
- C. Algorithmically shifting events to other indexes.
- D. Reingesting previously indexed data with new field names.

Answer: A

NEW QUESTION 249

- (Exam Topic 2)

The stats command will create a _____ by default.

- A. Table
- B. Report
- C. Pie chart

Answer: A

NEW QUESTION 250

- (Exam Topic 2)

A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

- A. One.
- B. Two.
- C. It depends on whether the original fields have the same name.
- D. It depends on whether the two sourcetypes are associated with the same index.

Answer: B

NEW QUESTION 251

- (Exam Topic 2)

Use the dedup command to _____.

- A. Rename a field in the index
- B. remove duplicate values
- C. provide an additional alias for the field that can
- D. be used in the search criteria

Answer: B

NEW QUESTION 256

- (Exam Topic 2)

Which of the following transforming commands can be used with transactions?

- A. chart, timechart, stats, eventstats
- B. chart, timechart, stats, diff
- C. chart, timeehart, datamodel, pivot
- D. chart, timecha:t, stats, pivot

Answer: A

Explanation:

The correct answer is A. chart, timechart, stats, eventstats.

Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways¹.

Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by using the transaction command or by creating a transaction type in the transactiontypes.conf file².

Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:

➤ chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics³.

➤ timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers⁴.

➤ stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields⁵.

➤ eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.

These commands can be applied to transactions by using the transaction fields as arguments. For example, if you have a transaction type named “login” that groups events based on the user field and has fields such as duration and eventcount, you can use the following commands with transactions:

➤ | chart count by user : This command creates a table or a chart that shows how many transactions each user has.

➤ | timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.

➤ | stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.

➤ | eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.

The other options are not valid because they include commands that are not transforming commands or cannot be used with transactions. These commands are:

➤ diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.

➤ datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.

➤ pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.

References:

➤ About transforming commands

➤ About transactions

➤ chart command overview

➤ timechart command overview

➤ stats command overview

➤ [eventstats command overview]

➤ [diff command overview]

➤ [datamodel command overview]

➤ [pivot command overview]

NEW QUESTION 260

- (Exam Topic 2)

The macro weekly sales (2) contains the search string: index=games | eval ProductSales = \$Price\$ * \$AmountSold\$

Which of the following will return results?

- A. 'weekly sales (3)'
- B. 'weekly_sales(\$3.995, \$108)'
- C. 'weekly_sales (3.99, 10)'
- D. 'weekly sales (3.99, 10)'

Answer: C

Explanation:

To use a search macro in a search string, you need to place a back tick character (``) before and after the macro name¹. You also need to use the same number of arguments as defined in the macro². The macro weekly sales (2) has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.

The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses spaces instead of commas to separate the argument values.

Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

NEW QUESTION 261

- (Exam Topic 2)

Which tool uses data models to generate reports and dashboard panels without using SPL?

- A. Visualization tab
- B. Pivot
- C. Datasets
- D. splunk CIM

Answer: B

Explanation:

The correct answer is B. Pivot¹.

In Splunk, Pivot is a tool that uses data models to generate reports and dashboard panels without the need for users to write or understand Splunk's Search Processing Language (SPL)¹. Data models enable users of Pivot to create compelling reports and dashboards¹. When a Pivot user designs a pivot report, they select the data model that represents the category of event data that they want to work with¹. Then they select a dataset within that data model that represents the specific dataset on which they want to report¹. This makes Pivot a powerful tool for users who need to create visualizations but do not have a deep understanding of SPL¹.

NEW QUESTION 263

- (Exam Topic 2)

which of the following commands are used when creating visualizations(select all that apply.)

- A. Geom
- B. Choropleth
- C. Geostats
- D. iplocation

Answer: ACD

Explanation:

The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are:

➤ geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions.

➤ geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters.

➤ iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

NEW QUESTION 266

- (Exam Topic 2)

When used with the timechart command, which value of the limit argument returns all values?

- A. limit=*
- B. limit=all
- C. limit=none
- D. limit=0

Answer: D

Explanation:

The correct answer is D. limit=0. This is because the limit argument specifies the maximum number of series to display in the chart. If you set limit=0, no series filtering occurs and all values are returned. You can learn more about the limit argument and how it works with the agg argument from the Splunk documentation¹. The other options are incorrect because they are not valid values for the limit argument. The limit argument expects an integer value, not a string or a wildcard. You can learn more about the syntax and usage of the timechart command from the Splunk documentation²³.

NEW QUESTION 271

- (Exam Topic 2)

Calculated fields can be based on which of the following?

- A. Tags
- B. Extracted fields
- C. Output fields for a lookup
- D. Fields generated from a search string

Answer: B

Explanation:

"Calculated fields can reference all types of field extractions and field aliasing, but they cannot reference lookups, event types, or tags."

NEW QUESTION 273

- (Exam Topic 2)

Which search retrieves events with the event type web_errors?

- A. tag=web_errors
- B. eventtype=web_errors
- C. eventtype "web errors"
- D. eventtype (web_errors)

Answer: B

Explanation:

The correct answer is B. eventtype=web_errors.

An event type is a way to categorize events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports¹.

To search for events that have a specific event type, you need to use the eventtype field with the name of the event type as the value. The syntax for this is:

eventtype=<event_type_name>

For example, if you want to search for events that have the event type web_errors, you can use the following syntax:

eventtype=web_errors

This will return only the events that match the search criteria defined by the web_errors event type.

The other options are not correct because they use different syntax or fields that are not related to event types. These options are:

- A. tag=web_errors: This option uses the tag field, which is a way to add descriptive keywords to events based on field values. Tags are different from event types, although they can be used together. Tags can be used to filter and group events by common characteristics².
- C. eventtype "web errors": This option uses quotation marks around the event type name, which is not valid syntax for the eventtype field. Quotation marks are used to enclose phrases or exact matches in a search³.
- D. eventtype (web_errors): This option uses parentheses around the event type name, which is also not valid syntax for the eventtype field. Parentheses are used to group expressions or terms in a search³.

References:

- About event types
- About tags
- Search command cheatsheet

NEW QUESTION 277

- (Exam Topic 2)

_____ datasets can be added to root dataset to narrow down the search

- A. parent
- B. extracted
- C. event
- D. child

Answer: D

Explanation:

Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.

NEW QUESTION 278

- (Exam Topic 2)

Which of the following statements describes an event type?

- A. A log level measurement: info, warn, error.
- B. A knowledge object that is applied before fields are extracted.
- C. A field for categorizing events based on a search string.
- D. Either a log, a metric, or a trace.

Answer: C

Explanation:

This is because an event type is a knowledge object that assigns a user-defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards. You can learn more about event types from the Splunk documentation¹. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

NEW QUESTION 280

- (Exam Topic 2)

A macro has another macro nested within it, and this inner macro requires an argument. How can the user pass this argument into the SPL?

- A. An argument can be passed through the outer macro.
- B. An argument can be passed to the outer macro by nesting parentheses.
- C. There is no way to pass an argument to the inner macro.
- D. An argument can be passed to the inner macro by nesting parentheses.

Answer: D

Explanation:

The correct answer is D. An argument can be passed to the inner macro by nesting parentheses.

A search macro is a way to reuse a piece of SPL code in different searches. A search macro can take arguments, which are variables that can be replaced by different values when the macro is called. A search macro can also contain another search macro within it, which is called a nested macro. A nested macro can also take arguments, which can be passed from the outer macro or directly from the search string.

To pass an argument to the inner macro, you need to use parentheses to enclose the argument value and separate it from the outer macro argument. For example, if you have a search macro named `outer_macro` (1) that contains another search macro named `inner_macro` (2), and both macros take one argument each, you can pass an argument to the inner macro by using the following syntax:

```
outer_macro (argument1, inner_macro (argument2))
```

This will replace the `argument1` and `argument2` with the values you provide in the search string. For example, if you want to pass "foo" as the `argument1` and "bar" as the `argument2`, you can write:

```
outer_macro ("foo", inner_macro ("bar"))
```

This will expand the macros with the corresponding arguments and run the SPL code contained in them. References:

- [Search macro examples](#)
- [Use search macros in searches](#)

NEW QUESTION 284

- (Exam Topic 2)

Which of the following is true about the Splunk Common Information Model (CIM)?

- A. The data models included in the CIM are configured with data model acceleration turned off.
- B. The CIM contains 28 pre-configured datasets.
- C. The CIM is an app that needs to run on the indexer.
- D. The data models included in the CIM are configured with data model acceleration turned on.

Answer: D

Explanation:

The Splunk Common Information Model (CIM) is an app that contains a set of predefined data models that apply a common structure and naming convention to data from any source. The CIM enables you to use data from different sources in a consistent and coherent way. The CIM contains 28 pre-configured datasets that cover various domains such as authentication, network traffic, web, email, etc. The data models included in the CIM are configured with data model acceleration turned on by default, which means that they are optimized for faster searches and analysis. Data model acceleration creates and maintains summary data for the data models, which reduces the amount of raw data that needs to be scanned when you run a search using a data model.

Splunk Core Certified Power User Track, page 10. : Splunk Documentation, About the Splunk Common Information Model.

NEW QUESTION 288

- (Exam Topic 2)

Which of the following expressions could be used to create a calculated field called gigabytes?

- A. `eval sc_bytes(1024/1024)`
- B. `| eval negabytes=sc_bytes(1024/1024)`
- C. `megabytes=sc_bytes(1024/1024)`
- D. `sc_bytas(1024/1024)`

Answer: B

NEW QUESTION 289

- (Exam Topic 2)

Why would the following search produce multiple transactions instead of one?

```
index=security sourcetype=linux_secure failed earliest=-60d@d latest=-1d@d
| transaction src_ip
| stats list(eventcount) as num_events sum(eventcount) as total_events by src_ip
```

Events (641) Patterns **Statistics (147)** Visualization

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 Next >

src	num_events	total_events
107.3.146.207	1000 1000 1000 405	3405
108.65.113.83	1000 120	1120
109.169.32.135	1000 1000 79	2079
11.17.160.129	1000 1000 238	2238

- A. The maxspan option is not included.
- B. The transaction command has a limit of 1000 events per transaction.
- C. The transaction and commands cannot be used together.
- D. The stats list () function is used.

Answer: A

Explanation:

The correct answer is A. The maxspan option is not included1.

In Splunk, the transaction command is used to group events that share common characteristics into a single transaction1. By default, the transaction command groups all matching events into a single transaction1.

However, you can use the maxspan option to limit the time span of the transactions1. If the time span between the first and last event in a transaction exceeds the maxspan value, the transaction command will start a new transaction1.

Therefore, if the maxspan option is not included in the search, the transaction command might produce multiple transactions instead of one if the time span between the first and last event in a transaction exceeds the default maxspan value1.

Here is an example of how you can use the maxspan option in a search:

```
index=main sourcetype=access_combined | transaction someuniquefield maxspan=1h
```

In this search, the transaction command groups events that share the same someuniquefield value into a single transaction, but only if the time span between the first and last event in the transaction does not exceed 1 hour1. If the time span exceeds 1 hour, the transaction command will start a new transaction1.

NEW QUESTION 290

- (Exam Topic 2)

What is the correct format for naming a macro with multiple arguments?

- A. monthly_sales(argument 1, argument 2, argument 3)
- B. monthly_sales(3)
- C. monthly_sales[3]
- D. monthly_sales[argument 1, argument 2, argument 3]

Answer: C

Explanation:

The correct format for naming a macro with multiple arguments is monthly_sales3. The square brackets indicate that the macro has arguments, and the number indicates how many arguments it has. The arguments are separated by commas when calling the macro, such as monthly_sales[region,salesperson,date].

NEW QUESTION 295

- (Exam Topic 2)

Which of the following searches will return all clientip addresses that start with 108?

- A. ... | where like (clientip, "108.%)
- B. ... | where (clientip, "108. %")
- C. ... | where (clientip=108. %)
- D. ... | search clientip=108

Answer: A

NEW QUESTION 297

- (Exam Topic 2)

What is the correct way to name a macro with two arguments?

- A. us_sales2
- B. us_sales(1,2)
- C. us_sale,2
- D. us_sales(2)

Answer: D

NEW QUESTION 300

- (Exam Topic 2)

Clicking a SEGMENT on a chart, _____.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 301

- (Exam Topic 2)

During the validation step of the Field Extractor workflow: Select your answer.

- A. You can remove values that aren't a match for the field you want to define
- B. You can validate where the data originated from
- C. You cannot modify the field extraction

Answer: A

Explanation:

During the validation step of the Field Extractor workflow, you can remove values that aren't a match for the field you want to define². The validation step allows you to review and edit the values that have been extracted by the FX and make sure they are correct and consistent². You can remove values that aren't a match by clicking on them and selecting Remove Value from the menu². This will exclude them from your field extraction and update the regular expression accordingly². Therefore, option A is correct, while options B and C are incorrect because they are not actions that you can perform during the validation step of the Field Extractor workflow.

NEW QUESTION 303

- (Exam Topic 2)

If there are fields in the data with values that are " " or empty but not null, which of the following would add a value?

- A. | eval notNULL = if(isnull (notNULL), "0" notNULL)
- B. | eval notNULL = if(isnull (notNULL), "0"
- C. | eval notNULL = "" | nullfill value=0 notNULL
- D. | eval notNULL = "" fillnull value=0 notNULL

Answer: D

Explanation:

The correct answer is D. | eval notNULL = "" fillnull value=0 notNULL

- Option A is incorrect because it is missing a comma between the "0" and the notNULL in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option B is incorrect because it is missing the false_value argument in the if function. The correct syntax for the if function is if (condition, true_value, false_value).
- Option C is incorrect because it uses the nullfill command, which only replaces null values, not empty strings. The nullfill command is equivalent to fillnull value=null.
- Option D is correct because it uses the eval command to assign an empty string to the notNULL field, and then uses the fillnull command to replace the empty string with a zero. The fillnull command can replace any value with a specified replacement, not just null values.

NEW QUESTION 306

- (Exam Topic 2)

Where are the results of eval commands stored?

- A. In a field.
- B. In an index.
- C. In a KV Store.
- D. In a database.

Answer: A

Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/SearchReference/Eval>

The eval command calculates an expression and puts the resulting value into a search results field.

- If the field name that you specify does not match a field in the output, a new field is added to the search results.
- If the field name that you specify matches a field name that already exists in the search results, the results of the eval expression overwrite the values in that field.

NEW QUESTION 311

- (Exam Topic 2)

Which of the following describes the | transaction command?

- A. It is an SPL command that groups at least two events together based on shared values in selected fields.
- B. It allows an exchange of data from one Splunk index to another Splunk index.
- C. It is an SPL command that groups events together with shared values in selected fields.
- D. It allows an exchange of data from one Splunk system to another Splunk system.

Answer: C

Explanation:

- The transaction command is a Splunk command that finds transactions based on events that meet various constraints .
- Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member .
- The transaction command groups events together by matching one or more fields that have the same value across the events . For example, | transaction clientip will group events that have the same value the clientip field.

NEW QUESTION 316

- (Exam Topic 2)

which of the following are valid options with the chart command

- A. useother
- B. usenull
- C. fillfield
- D. usefiled

Answer: AB

NEW QUESTION 321

- (Exam Topic 2)

The time range specified for a historical search defines the _____.-----questionable on ans

- A. Amount of data shown on the timeline as data streams in
- B. Amount of data fetched from index matching that time range
- C. Time range for the static results

Answer: B

Explanation:

The time range specified for a historical search defines the amount of data fetched from the index matching that time range². A historical search is a search that runs over a fixed period of time in the past². When you run a historical search, Splunk searches the index for events that match your search string and fall within the specified time range². Therefore, option B is correct, while options A and C are incorrect because they are not what the time range defines for a historical search.

NEW QUESTION 326

- (Exam Topic 2)

Which of the following statements would help a user choose between the transaction and stats commands?

- A. state can only group events using IP addresses.
- B. The transaction command is faster and more efficient.
- C. There is a 1000 event limitation with the transaction command.
- D. Use state when the events need to be viewed as a single event.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction>

One of the statements that would help a user choose between the transaction and stats commands is that there is a 1000 event limitation with the transaction command³. The transaction command is used to group events that share a common value for one or more fields into transactions³. The transaction command has a default limit of 1000 events per transaction, which means that it will not group more than 1000 events into a single transaction³. This limit can be changed by using the maxevents parameter, but it can affect the performance and memory usage of Splunk³. Therefore, option C is correct, while options A, B and D are incorrect because they are not statements that would help a user choose between the transaction and stats commands.

NEW QUESTION 328

.....

Relate Links

100% Pass Your SPLK-1002 Exam with Exam Bible Prep Materials

<https://www.exambible.com/SPLK-1002-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>